The Council of the Central Laboratory of the Research Councils (CCLRC)

Computer and Networks Security Group

Information Systems Privacy and Security Policy

Issue 2.0

July 2002

Contents

Foreword

The Policy Statement

The Council of the Central Laboratory of the Research Councils (the CCLRC), like all other non-departmental public bodies, is required by H. M. Treasury to define, document and implement an IS Security Policy.

*There is also a statutory requirement under the Data Protection Act 1998 (DPA '98) to protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to personal data. The seventh Principle of DPA '98 requires '**Appropriate technical and organisational measures to be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data**'.*

The CCLRC's dependency on computer systems, the sensitivity of much of the data held and the use of local and wide area networks, including the Joint Academic Network (JANET), make it important that a comprehensive security policy covering the CCLRC's information systems is documented and disseminated to all staff, especially those with responsibility for information systems (IS).

In defining this policy, the CCLRC has called upon the experience of other comparable organisations and has taken into account guidelines issued by H. M. Treasury, The National Computer Centre and, particularly, the British and the International Standards Institutes.

As an HMG body the CCLRC is required to have a security policy which gives appropriate protection against compromise to official information. The CCLRC has very few assets which are protectively marked RESTRICTED, CONFIDENTIAL, SECRET or TOP SECRET and this policy document does not therefore attempt to fully cover protection of such assets. Where classified information is held on computer all the rules in this document will apply, plus the rules contained in the HMG Infosec Standard (Chapter 5 of the Manual of Protective Security available on a need to know basis from the DSO).

Principles and Approach

The main business of the CCLRC is to promote research, to support the advancement of knowledge and to promote public understanding in science, engineering and technology. This involves close collaboration with a wide variety of academic and research institutes and technological companies world-wide, and a free exchange of information with both these organisations and the general public is a fundamental part of most of the CCLRC's work.

The facilities offered by the Internet are essential to meet these requirements for collaboration and dissemination, but they can be exploited only by operating a relatively open internet security policy which permits those facilities to be deployed to full advantage.

The Policy therefore cannot be to attain complete and guaranteed Internet security: to attempt to do so would necessarily impose unacceptable restrictions on the way the CCLRC discharges its primary responsibilities. It is rather to find ways of achieving adequate Internet security while permitting the work of the Laboratory to proceed relatively unimpeded. It is a compromise: it is a balance.

Other considerations of the Policy are similar to those of most other organisations.

The Development of the Policy

The initial version of the Policy was drafted by CNSG and adopted in July 1999 by the Laboratory Management Board, following consultation with RCIAS. It was based on the recommendations in BS 7799.

The Policy was extensively revised early in 2002 to take into account various technological developments, particularly those concerning portables, home computers and wireless networking, to accommodate experience gained from operating the Policy, to cover the new RIP Act, and to comply with ISO 17799.

It was endorsed by RCIAS at the meeting of Audit Committee on 19 June 2002 and adopted by Corporate Management Board on 27 June 2002.

Intended Audience

This Policy is primarily intended for day-to-day use by all CCLRC staff with Information System responsibilities. All such staff are required to act upon and implement all the provisions of this Policy which apply to them or to the systems they manage.

It is also intended for use by CNSG to assist its deliberations and to help in deciding its actions. It defines the policy which CNSG is charged with implementing.

Finally, several sections of the Policy are directed at all CCLRC staff and contractors working on CCLRC premises, and all such persons are required to read the document and act in accordance with the sections which apply to them.

Related Documents

References to related documents can be found in Annex 2: Useful References and Web sites

This document defines the formal IS security policy. A companion document covers the procedures to be followed when an IS security incident occurs.

A closely related area is that of Risk Management. The Laboratory operates a Risk Committee to oversee the implementation of the Risk Management Working Group Report.

Section 1: Organisation

1.1 Introduction

The Policy outlined in this document covers physical and logical access to CCLRC's computing facilities and the maintenance of the services provided by them. It seeks to define the standards and best/ethical practices for the control of privacy, security and continuing availability in CCLRC information systems and also to identify those practices which may constitute abuse.

The policy also seeks to draw attention to those operational controls which reduce the risk of misuse, including abuse by authorised users.

The policy applies to ALL computing facilities within CCLRC and ALL authorised users of those facilities, whether or not these facilities are supported by the Council's Business and Information Technology Department, and whether or not they are classified as supporting management, administrative or scientific work. Where the policy differs for the different types of system this is indicated in the text.

1.2 Definition of Security

Computer security involves confidentiality, integrity of data and availability of systems. A secure system should:

- prevent the disclosure of information to anyone who is not authorised to receive it;
- prevent unauthorised modification or deletion of data;
- maintain the continuing integrity of information stored in it;
- hold information readily available for use by its legitimate users; and
- allow rapid and complete recovery from disasters.

Security means more than merely preventing unauthorised access: security should also be proactive - ensuring that systems and data are available for use when required by authorised users and that data integrity is preserved. Security of information systems must also ensure the provision of adequate education, training and management of staff in order to preserve the organisation's ability to carry out the desired processing competently.

1.3 Definition of Terms

The following terms have special meaning throughout this document.

Information System:

Any working computer or networking system owned by CCLRC or under CCLRC's control which is capable of storing and/or processing information.

IS Security Officer

The individual named as the IS Security Officer or, in his absence, his named deputy. See *Annex 3: Current Security Personnel*

System Administrator

Any person who is responsible for controlling the set-up or installation or continued operation of an information system.

User

Any person, whether a CCLRC employee or not, who has been authorised to use any information system owned by or under the control of CCLRC. Note this implies there can be no legitimate *un*authorised users of CCLRC's information systems.

1.4 Purpose of Policy

IS security policy is designed to:

- protect CCLRC from inadvertent risks and risks taken knowingly but ill-advisedly;
- protect CCLRC's business by eliminating weaknesses in the security of information and associated operational systems;
- provide relevant officers and CCLRC staff in general with information on how to reduce risks to a minimum;
- encourage CCLRC staff to maintain an awareness of best security practice in other organisations to ensure CCLRC's systems and data remain optimally protected;
- maintain the currency of guidelines and codes of conduct in order to keep abreast of emerging weaknesses and threats; and
- ensure systems are continually tested in a variety of ways and periodically audited to ensure that all appropriate measures are in place.

The policy addresses both technical and procedural issues, and sets those standards currently considered to be necessary. It represents the **minimum** action that should be taken in every CCLRC Department, Centre or other organisational unit.

1.5 Assumptions

It is assumed that all organisational units within CCLRC are capable of meeting the requirements of this Policy with respect to identifying the necessary responsible officers and carrying out the required duties. Throughout this document these are defined in terms of 'Department'. Organisational Units which are not Departments must either interpret all these requirements by analogy or arrange to be clearly and definitively associated with a Department for the purposes of maintaining IS Security. Thus it is a requirement that Centres and other autonomous organisational units such as the Directorate which cannot or do not wish to meet these requirements themselves obtain their representation on CNSG via the chosen associated Departmental IS Security Officer, and that officer and the associated

Department Head exercise their IS security responsibilities for all such bodies associated with them as if they were part of the Department. It is a requirement on the head of all non-departmental bodies to ensure one of these two arrangements is in place and is effective. In the remainder of this document any reference to Department includes all such bodies associated with the Department and applies by analogy to all units which have elected to act autonomously.

It is assumed that all CCLRC Departments will ensure they either have and maintain the appropriate expertise within their staff complement to carry out the requirements and recommendations contained herein, or to declare to the IS Security Officer that they do not have such expertise. In the latter case the IS Security Officer will make arrangements to provide the necessary expertise or advice, which assistance may be chargeable.

1.6 Scope

The CCLRC IS security policy applies to all information systems, the data they hold and their users, be they scientific, administrative or managerial, under CCLRC's control or direction. The security policy covers:

- CCLRC-owned, hired or leased computing and communications equipment, peripherals, and networks;
- equipment and networks located on CCLRC premises which are used or provided by other organisations with which CCLRC works closely, e.g. other research councils, higher educational institutions or UKERNA (the JANET network);
- software and programs;
- access to external databases and web material;
- data wherever and however it is held or transported; and
- CCLRC staff and other authorised users.

Departments will need to apply the policy and guidelines within the context of their own working practices and computer systems. Additional procedures, guidance and staff education may be necessary.

Section 2: Assets: Classification and Control

2.1 Classification of Assets

In order to prioritise the security measures to be put in place, all corporate information systems and data should be known and attributed a value in relation to the damage that could be caused in the event of a security violation. The impact of lost or damaged information or systems, or the effect of inappropriate disclosure or theft of information, on CCLRC business and personnel should be assessed according to the following guidelines:

IMPACT ON BUSINESS	DESCRIPTION
Low Impact	The inappropriate disclosure, theft or modification of data, or loss of data or processing facility would cause little or no damage to the organisation nor place personnel at risk of injury
High Impact	The inappropriate disclosure, theft or modification of data, or loss of data or processing facility would be damaging to the organisation or place personnel at risk of injury.

2.2 Protectively Marked Assets

Before any system that handles protectively marked assets (RESTRICTED, CONFIDENTIAL, SECRET or TOP SECRET) is brought into service the Manual of Protective Security requires that it is subject to Accreditation. Acting on the authority of the Departmental Security Officer (DSO), the Accreditor has to be satisfied that the information in his care will be properly safeguarded, and hence that all risk management assumptions are valid:

a) physical security is in place;

b) personnel have the required clearances;

c) procedure controls are laid down in a Security Operating Procedure and will be enforced;

d) any technical security measures can be relied upon.

2.3 Accountability for Assets

Hardware Inventory

An inventory must be prepared and maintained for all the Council's information systems. The inventory must include all PC's (including Laptops) on site and on loan at home, and all more substantial computing equipment.

General Inventory

Inventories must also be prepared and maintained for all other IS assets relating to High Business Impact systems including:

- Information assets (databases and data files, system documentation, manuals, continuity plans and contingency (disaster recovery) plans)
- Software assets (application software, system software, development tools and utilities)

It is the responsibility of Department Directors to ensure that all software installed on all information systems under their control is appropriately licensed and used within the constraints imposed by the supplier.

Section 3: Responsibility for Security

3.1 Roles and Responsibilities

CNSG

The Computer and Networks Security Group has the responsibility for devising and recommending IS security policy to CMB for approval and for subsequently implementing the policy as approved by CMB within CCLRC. Its members are the Departmental IS Security Officers and it is chaired by the CCLRC IS Security Officer. It reports via the Corporate Systems Technical and Operational Board (CSTOB) and the Corporate Systems Strategy Board (CSSB) to CMB. The Terms of Reference and current membership of CNSG are shown in *Annex 4: CNSG Terms of Reference and Membership*.

CCLRC Security Officer

The CCLRC Security Officer is formally responsible for all aspects of security on CCLRC premises. However, his responsibilities for IS security as defined in this policy statement cover only protectively marked assets.

CCLRC IS Security Officer

The CCLRC IS Security Officer has overall responsibility for ensuring that a CCLRC IS security policy is in place, is maintained and is being observed by all departments. In matters of routine IS security he reports to CMB via CSTOB and CSSB; in matters of direct threat to security he reports to and derives authority direct from the CEO. The current CCLRC IS Security Officer and his deputy is shown in *Annex 3: Current Security Personnel*.

Directors

Directors are responsible for Departmental IS security and for ensuring their Department follows CCLRC policy and implements the guidelines set out in this document. Directors will be ultimately answerable to the CCLRC Chief Executive Officer.

Departmental Security Officer (DSO)

Departmental Security Officer (DSO) is the Cabinet Office title for the person in each government department, agency, or NDPB responsible for security clearances and for the protection of protectively marked assets. In CCLRC this title and responsibility is held by the Head of General Administration.

The DSO is the formal point of contact with HM Government security agencies, including IS security agencies. In this document this post is always referenced by the acronym, 'DSO', to avoid confusion with the Departmental IS Security Officers.

Departmental IS Security Officers

Each Department must have a designated Departmental IS Security Officer. The current Officers are identified in *Annex 4: CNSG Terms of Reference and Membership*. Departmental IS Security Officers are *inter alia* responsible for:

- representing their department on CNSG;
- working actively with other members of CNSG to maintain the IS security of CCLRC;
- bringing recommended good practices to the attention of users within their department;
- reviewing security in the light of new developments, and liaising with other Departmental IS Security Officers as appropriate;
- identifying potential security gaps within their department and taking action to rectify them;
- monitoring exposure of IS assets to major threats;
- ensuring that appropriate departmental background monitoring and or transaction tracking is running on servers under their control at all times, analysing the results of the monitoring and tracking, and reporting as agreed;
- approving and advising on the security aspects of all major IT initiatives within their department;
- keeping the CCLRC IS Security Officer informed of all suspicious incidents and the actions taken to resolve them as and when they occur; and
- documenting and recovering from any security breaches which may occur.

If a security breach is suspected, the Departmental IS Security Officer will, as appropriate, disseminate relevant information within the Department, to other Departmental IS Security Officers and as appropriate, via the CCLRC IS Security Officer, report the circumstances to the Computer Emergency Response Team (CERT). In all cases the CCLRC IS Security Officer shall be notified immediately.

Systems Administrators

All information systems will require an administrator to undertake a range of tasks including adding or deleting users, ensuring that the system runs efficiently, ensuring that the system runs securely, managing change control where this is appropriate and resolving user queries. Procedures must be in place to ensure that Personnel Department or line managers notify the appropriate systems administrator immediately when staff leave CCLRC service or change their duties or responsibilities. Any action performed by any authorised user on any information system must always be traceable to an individual. In this respect "Temp" or guest accounts able to be used by several users over the same period of time should not normally be set up.

The root account on unix systems is a specific exception. In order to preserve continuity of service it is necessary that at least two system administrators have access to root. Note that logging on to root should rarely be necessary, however. Wherever possible, system administrator duties should be carried out under a personal account, acquiring root privileges from there as required.

System administration privileges on CCLRC computer and/or network equipment should only be granted to those individuals whose duties and responsibilities clearly require significant levels of access to computer and/or network operating systems. Individuals holding system administration privileges on these machines must be *bona fide* employees of CCLRC and/or trusted staff contracted by CCLRC. They must not be temporary staff. System Administrators must never abuse their rights and privileges, and must always follow the appropriate Administrators Code of Conduct where this has been specified. The NT Administrators' Code of Conduct is shown in *Annex 6: NT Administrators*

Code of Conduct, and in addition to being followed by all NT Administrators it should be used as an example of an Administrators’ Code of Conduct when specifying these for other systems.

By controlling user rights and the safeguards and software installed, System Administrators have the means to prevent unauthorised use of the systems under their control. System Administrators therefore carry the primary responsibility for ensuring the systems under their control are secure against unauthorised use. Although other safeguards against intruders may be in place elsewhere in the network these can never be completely reliable, especially if any other CCLRC system has already been compromised.

All System Administrators must be subscribed to the appropriate Hack-RAL or Hack-DL distribution list which are used for the dissemination of notices relating to security exposures. They must respond to the disseminated advice promptly and reliably.

Users must be formally authorised by Systems Administrators in writing as to the scope of their access to systems of High Business Impact, setting out in particular what the limits on their rights of access are, to ensure users do not inadvertently overstep their rights.

LAN Managers

LAN Managers (also known as 'Village Managers') are the persons within Departments at RAL authorised to manage their department's part of the LAN and to control users' access to it. This is a responsible and privileged duty, and LAN Managers carry much of the responsibility for the integrity and operation of the data network. Network support staff at DL and the local system administrator at Chilbolton carry the same responsibilities and duties at those sites.

All LAN Managers and their equivalents at DL and Chilbolton are required to follow the Code of Conduct laid out in Annex 12: LAN Managers' Code of Conduct.

Users

The first line of defence against systems and data corruption, abuse and misuse rests with the individual. Data is a valuable asset and must be adequately protected from unauthorised access, use or manipulation. All users of CCLRC computing facilities are personally responsible for ensuring the rights granted to them for accessing or modifying data are never misused, and for complying with data and copyright legislation applicable to commercial and personal data.

All users must be properly authorised in writing and must agree to abide by any terms and conditions imposed by that authorisation. In addition they must observe the Network Acceptable Use Policy set out in CCLRC Notices, the latest of which is reproduced in *Annex 8: Network Acceptable Use Policy*.

Passwords

Much of the IS security depends ultimately on the quality of the passwords controlling access to accounts and files. All users have the responsibility to formulate passwords in accordance with the guidance provided by IS Security Officers. In particular, passwords must not be able to be guessed easily or be easily crackable. Guidelines to good password creation are contained in *Annex 5: Guidance on Password Composition*. Passwords must never be divulged to others except as required by line management for ensuring continued access to essential data and processes. Passwords used by System Administrators must be chosen especially carefully, never divulged to others and changed immediately there is any possibility of others learning them.

User Knowledge

Users will need a basic understanding of the operation of computers in order to use them effectively and to take the necessary basic precautions to prevent unauthorised access and to safeguard data.

Security Training

Users must be trained so that they:

- are aware of the nature of IS security threats and concerns;

- can carry out simple procedures and respond appropriately, eg in the use of virus checking software;
- are able to understand and follow CCLRC's security policy in the course of their normal work; and
- can use IT facilities correctly.

Departmental IS Security Officers and line managers are responsible for providing or arranging necessary training and refresher courses.

Technical Staff

Technical staff will need to undertake a range of activities to ensure that systems are developed and maintained securely. These will include: running regular back-ups, applying all necessary security-related system patches and upgrades, managing access controls, diagnosing and correcting problems, dealing with password and access issues, monitoring user activity, logging problems, keeping abreast of technical developments and changes, dealing with contractors, etc.

Technical staff may need special privileges to carry out these tasks. Like Systems Administrators, Technical Staff must follow a code of practice designed to ensure those privileges are not abused. In particular, the privacy of data belonging to others must never be violated unless this is necessary for carrying out explicitly assigned duties. They must also be especially careful to ensure their passwords are well-chosen, uncrackable and carefully protected, as these passwords may control access to a wide range of information belonging to others.

Section 4: Physical and Remote Security

4.1 Physical and Environmental Security

In addition to general CCLRC security measures, information systems must be physically protected in a way commensurate with the risks. Special attention must be given to the risks of damage to accommodation, flooding, fire and electrical supplies. To protect against the latter, UPS systems should be considered for all critical servers.

Secure Areas

Physical security is based on the definition of clearly identifiable perimeters and is achieved through a series of strategically placed 'barriers' throughout the Council's premises. The levels of security at the perimeter are consistent with the value of the assets or services to be protected - in other words control is exercised at reasonable cost.

All servers, routers, gateways and other critical equipment should be housed within a suitably secure area. When unoccupied, the area should be secured and physically locked. Electronic surveillance should be considered in high risk environments.

Equipment Security

It is the responsibility of all council user staff to make sure that their PC or workstation is physically secured when not in use. Where practicable, rooms should be locked when not occupied.

Workstations must be logged out or protected with screen-saver security when unattended to prevent unauthorised access to systems, the Internet and email.

Physical Network Security

All wiring closets must be kept locked when unattended and access restricted to those personnel authorised by Departments to manage the equipment contained therein.

Wireless LANs

Wireless LANs offer the convenience of easy access to the LAN, but also expose the network to several risks. The principle risk is that an unapproved computer may be connected to the site LAN in a variety of ways without authorisation. To minimise this risk wireless LANs must be attached to the site LAN only with the prior approval of the CCLRC IS Security Officer. In general such approval will be granted only if the proposed networking arrangements are such as to ensure unapproved systems are connected as if they were outside the firewall. Known and approved systems may be connected to the internal LAN directly only if this can be achieved reliably and automatically in a way that cannot be subverted by unauthorised users.

4.2 Remote Security Considerations

Laptops

Equipment should not be removed from a site without appropriate authorisation and registration on the Laboratory's assets register. Laptops must be secured against abuse or theft when not in use. Where the data retained is of an *in confidence* or *personal* nature special care should be taken.

Managers and staff who have online access to the Council's systems from home or other locations off-site or who use portable equipment are to be regularly reminded of the impact of physical security on privacy (including those statutory responsibilities under the DPA'98) and logical security. Laptop users are to be warned, specifically, of their vulnerability to the risks of unauthorised disclosure, copyright and intellectual property rights violations described in other sections of this document, should their hardware be lost or stolen.

Laptops carried away from CCLRC premises are often connected to networks outside CCLRC's control, either directly or via an ISP. If this is to be done the laptop **must** be protected with all relevant security patches, a suitably configured personal firewall and a properly installed, maintained and up-to-date virus checker. If there is any suggestion that the laptop has been exposed to a danger of compromise it must be properly checked before it is reconnected to a CCLRC network.

Home Computers

Computers installed at home may be owned by CCLRC or the user. Whichever is the case, if they are to be used on Council business the same standards of security as those detailed above for laptops must be applied. Because they do not have the benefit of the protection mechanisms and regular maintenance available to computers on CCLRC's premises, and are possibly used for a wider range of purposes, they are especially vulnerable to compromise. It is the responsibility of the person using them for Council business to ensure these standards are maintained and Council property is not placed at risk either directly or via files generated on or transmitted through a home computer.

Personal Data

Personal or classified data stored on diskette, CD-ROM, backup media or even paper must be treated with the same care as personal data held on a hard drive or file-system. Data held on such media is more likely to be forgotten, lost, exposed to others, not declared, not registered or kept longer than is necessary. The Data Protection Act applies just as much to personal data on this type of media, and must be followed equally rigorously.

Network Connections and Modems

It is essential that all external network connections to the CCLRC network be properly controlled and monitored to prevent unauthorised intrusions. Any external network connection other than the main connection from the site to the Internet will permit security filters and monitoring to be bypassed. Such connections therefore represent a significant security exposure which must be controlled. Such connections include those provided by permanent circuits or transient dial-up connections using modems, ISDN or equivalents.

Permanent Connections

All permanent connections to any external site must be registered with and approved by the IS Security Officer. Normally this will be permitted only to meet scientific needs which cannot be satisfied using the normal JANET connection via the Internet, and connections will normally be permitted only to systems which are not connected to the CCLRC LAN.

Transient (Dialled) Connections

While these appear to present less risk as the connection to the Internet is usually of only short duration, the risks are nevertheless significant. While the connection is active the Internet connection established completely bypasses the security filters installed on the main connection to the Internet and search and compromise programs require only a few minutes to compromise a machine. Furthermore, open modem lines providing dial-in capability can be discovered by hackers with ease. Programs are readily available which try telephone numbers in a selected block looking for a modem response.

To control access, users and system administrators must not set up or provide dialled connections, either dial-in or dial-out, to any system connected to CCLRC's network without the prior permission of the CCLRC IS Security Officer, who will maintain a register of authorised dialled connections. Before granting permission to install such a facility he will need to be satisfied no security risk is being created. One condition of approval will be that any system providing dial-in capability must implement a user registration scheme and require a password to be provided before permitting access to the network. Dial-in systems other than the standard dial-in facility provided by BITD will not normally be permitted.

Dial-out only modems are less risky, especially if they are dialling to remote scientific systems which are not connected to the Internet, and this specific use will normally be permitted. However, such systems must still be registered so that the potential exposure arising from inadvertently mis-configuring them to provide a dial-in capability can be avoided by blocking incoming calls in the telephone exchange.

Note that modems connected to lap-tops are not required to be registered. However, users must not use the modem connection while the lap-top is directly connected to the CCLRC network.

Section 5: Computer and Network Management

Note: *There are a wide variety of computer systems within CCLRC and many of the generalisations detailed in this section may not be appropriate for all of them. Considerations as to which should apply should take into account a risk assessment and a cost/benefit analysis. If a decision is taken to disregard any part of these recommendations then the justification for doing so must be clearly recorded at the time the decision is taken and be held available for inspection in connection with audit at any later time.*

5.1 Networking Considerations

LAN

Most information systems owned by CCLRC are connected to the Local Area Network at either DL or RAL. At RAL these connections are controlled by the RAL LAN managers, and only LAN managers are authorised to make such connections. At DL LAN connections are controlled by the Network Support group within BITD according to agreements with the Departments at DL.

At Chilbolton the network is controlled by the local system administrator there.

A list of the current RAL LAN managers and the areas they control is shown in *Annex 9: RAL LAN* Managers.

RAL LAN Managers and their equivalents at DL and Chilbolton must follow the Code of Conduct laid out in Annex 12: LAN Managers' Code of Conduct.

JANET

CCLRC makes use of the Joint Academic Network (JANET) for data communication between its laboratories and other organisations. JANET is operated by UKERNA under the terms of a licence granted by OFTEL to the Secretary of State for Education and Employment and normal CCLRC activities fall within these terms.

JANET may be used by all legitimately connected organisations for all legal activities, including commercial activities, provided the JANET Acceptable Use Policy is observed. This is reproduced at *Annex 8: Network Acceptable Use Policy.*

When necessary and where cost effective CCLRC may use encryption technology for some of its data exchange activities.

Electronic Mail

Electronic mail and attachments are an important means of communication for CCLRC and offer facilities which are complementary to other media. However, they are no more secure than ordinary paper mail: email may be wrongly delivered, intercepted and/or forged. In addition, for legal purposes messages sent via email are considered a 'public disclosure', and sensitive information should not, therefore, be sent by this route unless the messages are strongly[*] encrypted.

Users should also be aware of other dangers of email. It is common for the language used in email to be relatively informal, yet emails are still legally binding. Also, any defamatory statements made in emails may result in court action against CCLRC or the individual sender. Finally, copyright material must not be used in emails any more than it may be used in publications without the permission of the copyright owner.

As a small measure of protection against misdirection, interception, copyright violation or defamation, users are strongly advised to attach a disclaimer to email being sent off-site which says either that the contents are confidential and for the use of the intended recipient only, or that the contents are not attributable to CCLRC, whether or not encryption is being used. Examples of suitable disclaimers are shown in *Annex 10: Email Postscripts*

Internet

Exporting information to the web and other Internet sites and importing data from them needs to be undertaken with great care and in the light of the advice given in this document. CCLRC web servers must have good security to prevent unauthorised editing or destruction of pages.

Software available on the Internet

Much software of value is available for download from the Internet, and a considerable part of CCLRC's normal work relies on such software. Users must always be aware, however, that downloading software carries risks of installing at the same time potentially damaging viruses or 'back doors'. These latter may provide ways in which hackers can gain access to CCLRC's computers. These risks will always be present and the guidelines here are intended only to minimise the risk, not eliminate it. Users should:

- never download games software onto CCLRC computers (these are especially risky);
- download software only from trusted sources;
- download only software that is required for carrying out CCLRC duties;
- always run a virus checker on downloaded software before installing it.

Firewall protection

Firewalls are designed to make sure that systems protected by them can only be accessed by authorised users. They can also be used to restrict access to the Internet for those who work behind them. The high degree of electronic collaboration with other organisations required to carry out CCLRC's normal work prevents the employment of the full protection of firewalls, but those facilities which can be employed without compromising CCLRC's normal work should be used. The following should be provided as a minimum:

- access to and from undesirable IP addresses should be prevented;
- the use of undesirable protocols should be prevented;
- network use should be monitored to detect intrusions and attempts at intrusion;
- network use should be monitored to detect violations of acceptable use policy.

[*] In this context 'strongly' means using an encryption technique which, at the time of sending, cannot feasibly be broken.

In addition, all incoming and outgoing email must be routed through a well-maintained virus checker; all http accesses to external webs must be via a controlled proxy server, and it is the intent that control over all other external accesses to internal interactive servers will be progressively strengthened by adopting a secure protocol such as ssh or by routing access via a proxy which implements such a secure protocol.

All servers providing access to external users will be given an IP address in the designated range to facilitate the protection of other systems not required to provide external access. The protection afforded to the site at large from (potentially compromised) externally visible servers will be progressively strengthened by technical improvements approved by CNSG.

All access to CCLRC's internal networks from off-site, and all restrictions on such access, however they may be implemented, are under the sole control of the CCLRC IS Security Officer and staff designated by him. General restrictions on access will be agreed before implementation by CNSG, but specific operational restrictions in response to a perceived security threat will be implemented by the CCLRC IS Security Officer or staff designated by him acting on their own authority.

The IS Security Officer will periodically arrange for an independent test or audit of the firewall protection to ensure potential exposures have not been overlooked.

5.2 Good Housekeeping

Maintenance of service

In order to maintain integrity and availability of service:

- operational procedures for all High Impact systems should be documented fully and contain up-to-date instructions;
- routine procedures must be established for all High Impact system back-ups, event and fault logging, system performance monitoring and change control;
- mirroring of servers should be considered;
- back-ups of High Impact servers should be made at appropriate intervals, daily is recommended, and backups should be stored in a locked fireproof safe or a copy locked away in a separate building;
- a log should be kept of the security features/upgrades that have been implemented or need to be implemented for each system or type of system that is accessible from off-site in order to minimise the risk of these being overlooked when the system is next upgraded;
- adequate provision must be made for deputising for all system administrators so that systems can be properly administered at all times, including times of unforeseen emergency; and
- means should be provided whereby individual users can back-up their important files.

Business Continuity

Contingency plans for preserving business continuity in the event of serious failure, for example a fire, should be in place as an essential part of the installation and operation of all High Impact systems. These plans should be designed to enable all the essential functionality to be re-established in an acceptable way within an acceptable time should the primary service become unavailable for an extended period. They may range from a simple set of desk procedures describing a manual method of providing the essential functionality to a comprehensive disaster recovery plan involving a fully equivalent backup service, depending on the nature and importance of the service. It is vital that the effect of loss of data is considered.

The plans should also include the procedures required to access or recover essential data both during the emergency interim arrangements and for the re-establishment of the full service. This may have implications for the way data is entered into the system in normal operation, the way records of data entry are generated and preserved, and the way data is backed up, all of which must be taken into account in the normal operating procedures.

5.3 Incident Management

Incident management procedures

If any system containing protectively marked data has been, or is suspected of having been, compromised in any way then a report should be made immediately to the DSO.

Incident management procedures have been documented and are available to all staff on the intranet. See Annex 2: Useful References and Web sites. All System Administrators should be familiar with them.

In order to allow recovery from incidents efficiently, the following additional requirements are recommended for all High Impact systems:

- procedures for responding to all types of potential security incidents, including system failures, errors and breaches of confidentiality, should be fully documented;
- if an intrusion is suspected, audit trails and similar evidence must be collected and secured as appropriate; this will almost certainly require the prior preparation of a tailored incident response tool-kit to quickly and reliably extract information about the executing system before it is closed down;
- responsibility for taking or organising action to correct and recover from a particular individual security breach or system failure should be clearly assigned to one person who should then carefully control the steps of the investigation and recovery;
- all suspected intrusions must be reported immediately to the CCLRC IS Security Officer via the appropriate Departmental IS Security Officer.

Viruses

No scheme can ensure 100% protection against viruses which may be brought into CCLRC via diskettes (and less often CDs), through email attachments or downloaded through documents and programs from the Internet. Servers as well as workstations need protecting. The aim of the following advice is to:

- minimise the risk of a virus reaching any CCLRC system, and
- ensure that any virus which is contracted is detected early and dealt with quickly and efficiently.

All diskettes and CDs being imported from outside CCLRC must be checked before use by a recommended up-to-date virus checking program. In addition, all systems, and parts of systems, must be protected by up-to-date anti-virus software which should be kept running at all times.

It is a requirement that all mail transfer agents which receive mail directly from the Internet are equipped with at least one up-to-date virus scanner to minimise the possibility of email-borne viruses and Trojan horses being carried into CCLRC. This should be a different scanner to the one in use on client systems to further improve the detection of viruses.

If users believe they have a virus on their equipment, they should immediately stop activity, disconnect the equipment from the network, and report to the Departmental IS Security Officer. Any single virus report may be just the "tip of the iceberg" of a more widespread infection. If there is a likelihood of a virus spreading, it will be necessary to broaden the investigation. In extreme cases, it may be necessary to call for a shut down of all systems and complete scanning of all data. A common reason for a first outbreak turning into a long-term chronic problem is ill-informed attempts to deal with the problem by non-expert staff. It is important that matters are dealt with in a calm, orderly manner. It is easy to destroy useful information before it has been recorded and make matters worse.

System Intrusions

All systems attached to the CCLRC internal network are also connected to the Internet and are therefore vulnerable to unauthorised intrusions from hackers. All possible precautions must be taken to prevent unauthorised access being gained in the first place, as once a system is compromised it becomes much harder to prevent the intrusion spreading to other systems. System administrators must always:

- ensure they are registered on the appropriate CCLRC security distribution list and read and act on disseminated information promptly;
- ensure all the latest security patches and upgrades are promptly applied to all the systems under their control, unless there are strong and justifiable reasons for not doing so;
- monitor systems as appropriate for intrusions; for all externally visible systems this monitoring should raise alerts automatically wherever possible (eg by periodically checking modification dates or hashed signatures of selected critical files);
- report all intrusions and suspected intrusions to the CCLRC IS Security Officer via the appropriate Departmental IS Security Officer;
- act promptly on any instruction given in connection with a security incident by the CCLRC IS Security Officer, including instructions to disconnect or switch off any system.

Responding to incidents

All security incidents which carry the possibility of a compromised system must be reported immediately they are detected to the CCLRC IS Security Officer. As much detail as possible should be given at the time of this reporting as this may hasten the recovery from the incident.

5.4 System Audits

Security reviews of Information Systems

Regular reviews of IS and data security must be undertaken by departments to ensure compliance with the security policies and standards set out herein.

Internal system audits

All Departments will be subject to periodic internal audits of the systems rated High Business Impact by a team comprising the CCLRC IS Security Officer and two independent Departmental IS Security Officers to ensure compliance with this Policy. The Audit Report will be submitted to the Department Head and CNSG. The Departmental response to the audit will be presented to CNSG at the following meeting.

External system audit considerations

From time to time various parts of CCLRC's information systems will be subject to external security audit by RCIAS or NAO. The CCLRC and appropriate Departmental IS Security Officers will act as the local contact for the auditors. Audit requirements and activities including checks on operational systems should be carefully planned and agreed with the auditors to minimise the risk of disruptions to business processes. The following should be observed:

- the scope and purpose of the audit must be agreed in advance with appropriate management;
- the precise checks and measurements must be agreed in advance and controlled;
- investigations by auditors should be limited to read only access;

- IT resources required for performing checks must be identified in advance and those agreed made available to auditors;
- requirements for special or additional processing should be identified and agreed with service providers;
- access to any system audit tools provided specially in order to conduct the audit must be safeguarded from unauthorised use, such tools should be kept separate from those installed as part of development and operational systems, and such tools must be disabled or removed at the completion of the audit.

5.5 System Development

Note: *This section on System Development applies to High Business Impact systems only.*

New systems

Statements of business requirements for new systems expected to be of High Business Impact must include details of security controls and these controls must reflect the value of the assets involved and the damage which might result from the absence or low levels of security.

Executable code

Executable code must not be put into productive use on any High Business Impact system without confirmation of correct operation by successful system and user acceptance tests. Back-out procedures in the event of unforeseen malfunctioning must also be put in place. These requirements should follow from the application of standard change control procedures.

Different arrangements may, however, be necessary for executable code used on High Impact systems in the research environment. In this case the procedures must be defined with respect to the relevant scientific and personnel safety requirements.

Test data

If copies of sensitive live data are involved, the following controls must be applied to protect the test data:

- access controls at the same level as those applied to live data must be applied to test data;
- there must be separate authorisation each time live data are copied to the test environment;
- live data must be irretrievably erased from the test application environment immediately after testing is complete;
- the copying of live data should be logged to provide an audit trail.

Change control

In order to minimise the potential for corruption of information systems, there should be strict control over the implementation of changes to systems classified as being of High Business Impact. Formal change control procedures must be put in place, so as to ensure that:

- security and control are not compromised;
- application programmers are given access only to those parts of the system that are necessary for their work;
- formal managerial approval is always obtained before any changes are made.

These procedures must include:

- measures to ensure that change requests are only accepted from users recognised to have such authority;
- a review of security controls to ensure that they will not be compromised by each change;
- the identification of all software, database files and hardware that require amendment;
- steps to ensure the user community is consulted on the desirability and timing of each change;
- measures to ensure that the system and user documentation is updated on the completion of each change.

Systems documentation

Full systems documentation, including latest versions of code, must be stored in a secure environment.

5.6 Disposal of Media holding Data

Data may be held on a computer's hard disk or on removable media such as diskettes, CD-Rs, CD-RWs, DVDs, etc and tapes of various types, collectively known as media. When the purpose for which a computer hard disk or media of any type is used is being significantly changed, or a computer or the media associated with it has come to the end of its useful life and is being discarded, the data held on those media should always be totally erased (if this is physically possible) or otherwise destroyed in order

a) to prevent the inadvertent transfer of licensed software in violation of the licence agreement,

b) to prevent the transfer or continued retention of personal data in a way which contravenes the Data Protection Act, and

c) to prevent the inadvertent transfer of protectively marked assets.

Section 6: System Access Control

6.1 Procedures and Controls

Confidentiality and non-disclosure

Under the terms of CCLRC employment a member of staff using CCLRC IS facilities must abide by the recognised rules of confidentiality and non-disclosure in relation to both information about systems and data on them. In addition, CCLRC staff may be required to sign agreements for access to information owned by organisations other than CCLRC. The terms of such agreements must be strictly observed.

The use of IS facilities by agency, temporary or contract staff should be covered by an appropriate CCLRC confidentiality agreement.

Authorisation

Appropriate CCLRC computing and networking resources should be available to all currently employed Council staff who need access to them for their everyday work. Managers have the responsibility of notifying systems administrators which of their staff should be given access, to what systems and data and under what circumstances. The level of access must be adequate but not excessive for the needs.

Up to date documentation on who has access to what data and what access rights they possess must be maintained by system administrators. When adding new users, system application forms (recording all access rights enjoyed by the individual) should be signed by both the member of staff that he/she understands access regulations and the system administrator who should clearly state whether the user id is temporary or permanent. If the user id is temporary, the expiry date should be specified.

It is strongly advised that all systems which invite logon via presentation of ID/Password inform the user of access restrictions in a banner display worded as follows:

"Access to this system is restricted to authorised personnel. If you do not have authorisation to access this system you should not proceed beyond this point and you should disconnect immediately."

IDs and Passwords

Users must have a valid user account name for each computer system they need to use, i.e. a user ID, and a password known only to that user. To prevent unauthorised use of systems, passwords must meet minimum standards of complexity to guard against their being guessed or cracked. Passwords must not be written down under any circumstances. Passwords may only be shared where there is no alternative and it is necessary to ensure business continuity in the event of staff absences.

All passwords should be tested against a password-cracking program such as CRACKER at intervals to ensure that user's passwords cannot be easily guessed.

Staff leaving or moving

Appropriate action must always be promptly taken by system administrators when a user of any system under their control no longer requires continuing access, or when the nature of that access may need changing due to a change of duties. In general, the appropriate action when a user leaves is to disable the account and to transfer any files to another nominated user account. If this is not possible the whole account should be transferred to another nominated user with a changed password.

Business requirement for system access

Each business application must have an owner who should maintain a clearly defined access policy. A confidentiality warning message must be displayed on entering all systems, e.g. "This system is for authorised users only. If in doubt contact your IT manager." A formal procedure for granting users access to systems containing restricted access data should be established to ensure a list of all individuals with access is known by the data owners. All System Administrators and all technical staff with access or with the potential to gain access must also be listed.

Access by agency or contract staff

Agency or contract staff need access to systems and data from time to time. Such access must be appropriately authorised. A record of who is being given access, for how long, for what purposes and to what systems should be placed on file by an appropriate, responsible member of CCLRC staff.

Non-CCLRC staff should be routinely monitored to ensure that they are meeting their security obligations.

Security of Third Party Access

On occasions third party access will be required by agencies not contractually associated with CCLRC. Sometimes the police or another government agency may be involved, especially if CCLRC equipment has been used to gain unauthorised access to other organisations' facilities or vice versa..

The CCLRC IS Security Officer must always be advised of such cases. In general, CCLRC management and staff are expected to be as helpful as possible while avoiding disclosure of information which would place the security of CCLRC's facilities further at risk. Staff are reminded that they must not disclose any sensitive/personal data without first establishing the *bona fides* of the person requesting information and being sure that the disclosure (in relation to personal data) is permitted by CCLRC's data protection registration - especially when requests are received by e-mail or public telephone. The wisdom of not taking such requests at face value must be emphasised; managers and staff should always confirm that an inquiry does originate from the organisation or agency the caller claims to represent.

Section 7: Legislation and Compliance

7.1 Data Protection Act

The storage and use of computerised [and certain manual] records relating to individuals is governed by the Data Protection Act (DPA ’98). All staff processing information relating to living identifiable individuals including the obtaining, holding, use or disclosure of such information must make themselves aware of the requirements of DPA ’98. New processing of personal data must not commence without the knowledge and approval of the CCLRC Data Protection Officer.

DPA ’98 is surrounded by eight Data Protection Principles which must be adhered to. The Principles and some pertinent definitions are shown in *Annex 11: Data Protection Principles.*

Information relating to the Act can be obtained from the CCLRC Data Protection Officer.

7.2 Regulation of Investigatory Powers (RIP) Act

The pertinent points in this Act are summarised in Annex 13: The Regulation of Investigatory Powers (RIP) Act 2000. Together with the associated Regulations this Act limits the interception of telecommunications traffic to certain well-defined circumstances.

The main implications for CCLRC are that telephone and network traffic may not be lawfully monitored or recorded unless authorised, and that all reasonable efforts must be made to notify all users that monitoring may take place.

Authorisation of monitoring

The CCLRC IS Security Officer, the Deputy CCLRC IS Security Officer, the Department Security Officer (DSO) and the Departmental IS Security Officers are all hereby authorised *ex officio* to intercept communications on that part of the telecommunications system for which they are responsible in order

a) to establish the existence of facts to ascertain compliance with regulatory or self-regulatory practices or procedures;

b) to prevent or detect crime;

c) to investigate or detect unauthorised use of telecommunications systems;

d) to secure, or as an inherent part of, effective system operation.

This authorisation may be extended to further individuals by any of the named Officers. This extension must be given in writing, and must be both specific and time-limited. It cannot be issued retrospectively. A suitable form of authorisation is shown in Annex 14: Authority to Intercept

Communications. Copies of the Authorisation must be given to and retained by the person being authorised, the authorising person and the CCLRC IS Security Officer.

A request to monitor the communications of a specific individual must be sanctioned by either the Head of Human Resources or the Head of the Department to which the individual belongs or with which he is associated.

Members of staff, visitors and all other users of the CCLRC telecommunications systems must not intercept telecommunications messages unless they hold appropriate written authorisations to do so.

Notifying users that monitoring may occur

Interceptions made under the authority of the Telecommunications Regulations will only be lawful if the controller of the telecommunications system on which they occur has made all reasonable efforts to inform potential users that interceptions may be made.

Staff will be notified of this through this Policy document, and through periodic Notices issued to all staff. Users of computer systems will be notified when their accounts are created, and by an informatory notice presented to them whenever they logon.

Casual and unsolicited users (eg, those accessing web servers, ftp servers, sending email, etc) will be notified by messages on the main web pages and by a standard message added to all outgoing email.

In all cases the notice should take the form:

"CCLRC's telecommunications systems may be monitored in accordance with the policy available from *http://www.foi.cclrc.ac.uk/Activity/ACTIVITY=Monitoring*".

7.3 Use of Proprietary Software

Ultimately, individual Directors are responsible for ensuring that all proprietary software used by staff in their departments is correctly licensed.

Commercial software and databases are defined as "Intellectual Property" and are protected by the law. They are normally obtained from suppliers under the terms of an agreement, which defines the conditions under which they may be used. CCLRC requires all users to comply with the terms of licence agreements into which it has entered and not knowingly to use unauthorised copies of software. CCLRC staff should be aware that the CCLRC may be subject to a FAST (Federation Against Software Theft) audit at any time.

Some software and datasets used by CCLRC are obtained under Combined Higher Education Software Team (CHEST) licences or similar arrangements. Deals may be directly negotiated with the supplier or may be the result of negotiation by CHEST on behalf of the academic community. In order to simplify the process of negotiation with software suppliers, the JISC has agreed a Code of Conduct governing the use of software purchased under special academic terms. The business of CCLRC falls within the definition of academic use and normal computing activities in support of Council's activities comply with the Code.

Note that many licences for software in use in CCLRC cover academic use only. If software is to be used for non-academic purposes a suitable commercial licence must first be obtained.

Internal audits of the software installed on computer systems will be conducted periodically. Users must ensure they have documentary proof available that the software installed on their systems is properly licensed for use.

7.4 Discipline

Misuse of any CCLRC facility, including computing facilities, is a serious offence under the terms of the CCLRC CEMs. Any alleged misuse must be investigated in accordance with the disciplinary procedure and may render a member of staff liable to disciplinary action. Access may immediately be denied to anyone suspected of abusing computing facilities.

Misuse of any CCLRC facility, including computing facilities, by any non-staff users will be treated equally seriously and may result in the immediate withdrawal of access to the facility and to CCLRC premises.

7.5 Sanctions

If the recommendations set out in this document are persistently ignored in such a manner that (in the opinion of the CCLRC IS Security Officer) the security of CCLRC's information systems or data is placed at serious risk, then the CCLRC IS Security Officer may require that an individual computer or computers or an entire part of the LAN be disconnected from the main CCLRC network.

Appendix A: Annexes

Annex 1: Acronyms

CEO	Chief Executive Officer
CERT	Computer Emergency Response Team
CHEST	Combined Higher Education Software Team
CCLRC	Central Laboratory of the Research Councils
CMB	Corporate Management Board
CNSG	Computer and Network Security Group
CSSB	Corporate Systems Strategy Board
CSTOB	Corporate Systems Technical and Operational Board
DPA	Data Protection Act
DSO	Departmental Security Officer (a Cabinet Office title)
FAST	Federation Against Software Theft
IS	Information System
IT	Information Technology
JANET	Joint Academic Network
JISC	Joint Information Systems Committee
LAN	Local Area Network
NAO	National Audit Office
NISS	National Information Services and Systems
OFTEL	Office of Telecommunications
RCIAS	Research Councils' Internal Audit Service
RIP	Regulation of Investigatory Powers (Act)
UKERNA	UK Educational and Research Network Association
UPS	Un-interruptible Power Supply

Annex 2: Useful References and Web sites

Not all the Acts and Standards relevant to IS security are published in full-text form on the web. Where permitted, full text or summaries are provided locally in http://committees-www.clrc.ac.uk/is/cnsg/public/legislation Note that access will require a CCLRC federal ID and password.

The definitive version of this document is held at

- http://www-internal.clrc.ac.uk/staff/computing/security/issue2.0.doc

and a simple guide is available at

- http://www-internal.clrc.ac.uk/staff/computing/security/

The Incident Handling Guide is available at

- http://committees-www.clrc.ac.uk/is/cnsg/public/Incident Procedure/Issue_1.doc

Other useful references:

Risk Management

The CCLRC Working Group Report can be found at

- http://www-internal.clrc.ac.uk/staff/risk_management/

British Standards Institute - BS 7799 Code of Practice for Information Security Management

Not freely available on the web in full-text form but may be accessed via the Library at

- http://www-internal.clrc.ac.uk/staff/library/

for registered users. For summaries see

- http://committees-www.clrc.ac.uk/is/cnsg/public/BS 7799/bs7799.htm
- http://www.c-cure.org/

ITSec Security and Evaluation Scheme

- http://www.cesg.gov.uk/assurance/iacs/itsec

Computer Misuse Act (1990)

The full text is available at

- http://www.hmso.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm

Copyright, Designs and Patents Act (1988)

The full text is available at

- http://www.hmso.gov.uk/acts/acts1988/Ukpga_19880048_en_1.htm

Data Protection Act 1998

The full text is available at

- http://www.hmso.gov.uk/acts/acts1998/19980029.htm

Regulation of Investigatory Powers (RIP) Act

The full text is available at

- http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Annex 3: Current Security Personnel

Chairman of CSSB	K J Peach
Chairman of CSTOB	K G Jeffery
CCLRC Security Officer	J J Hamilton
CCLRC IS Security Officer	T Daniels, *Deputy* P S Kummer
CCLRC Data Protection Officer	C Taylor
Departmental Security Officer (DSO)	J J Hamilton

Annex 4: CNSG Terms of Reference and Membership

Terms of Reference

The Computer and Network Security Group reports to CSTOB. CNSG is responsible for drafting and maintaining the Laboratory's Privacy, Security and Continuing Availability Policy for endorsement by CMB, and for overseeing its subsequent implementation on all CCLRC's computers and networks.

In particular, CNSG will

- consider all Internal Audit Reports of IS Security and act to implement the agreed recommendations;
- maintain a Privacy, Security and Continuing Availability Policy for endorsement by CMB covering all aspects of IS security, including all those in HMG's most recent IT Security Policy Statement, and in particular covering the requirements of the Data Protection Act, the Computer Misuse Act, the RIP Act and the guidance from the Federation Against Software Theft;
- oversee the implementation of the agreed Policy in all its aspects on a continuing basis, and establish the co-ordination required between departmental IS security officers to ensure a uniform and adequate implementation of the agreed security measures;
- report to CSTOB annually.

CNSG will be constituted to be representative of all the Laboratory's departments. Its chairman will be the IS Security Officer, normally the Head of e-Infrastructure in BITD, and all departments will provide a technical representative able to take technical decisions with respect to their department's computers and networks. Experts will be co-opted as required.

Membership

This membership table shows the nominated representatives and deputies as of July 2002.

DEPT	REPRESENTATIVE	DEPUTY
SSTD	Adrian Boulter	Dave Terrett
ENG	Mike Courthold	
BITD	Paul Kummer	Robin Tasker
ADM/FIN	Ken Hartley	Richard Owen
SRD/AST	Chris Dean	Mark Enderby
ISIS	Kevin Knowles	Bob Mannix; Richard Brodie
CLF	Chris Reason	Dave Peplar
CSE	David Laff	
ESC	Andrew Sansum	Nick Hill
PPD	Gareth Smith	Barry Saunders
INS	Nicky Watkins	Tony Lucas
RCD	Charles Kilburn	Adham Tamer
SND	Simon Letts	
Chairman	Trevor Daniels	Paul Kummer
Secretary	Neil Calton	Graham Robinson
Experts	Jerry Hopkinson Chris Seelig Chris Taylor (Data Prot Officer)	

Annex 5: Guidance on Password Composition

Introduction

This note provides advice and guidance on the generation of passwords and much of it is applicable to any computer system. So whilst it was written with NT users specifically in mind it is strongly recommended that all computer users read this note and implement its ideas.

CCLRC, along with many other sites, has experienced an increasing level of attack by hackers for some years. One of the more dangerous types of attack is one which enables an intruder to obtain passwords so that he can gain access to normal user or administrator accounts on our systems. Once an intruder can do this it is very difficult to detect the intrusion, which can then spread very rapidly to other systems. The only protection against this is the quality of the passwords used by users.

NT systems in their normal form do not permit telnet-like logins from anything other than the attached keyboard, but access can be gained to files on any networked NT system via any account which has access rights to those files. The only protection against unauthorised file access from anywhere on the network is the password. Bear in mind too that intruders are not necessarily external to CCLRC: many organisations have found that internal intruders are more of a problem.

Although NT passwords are usually stored and transmitted in encrypted forms there are very sophisticated password cracking programs freely available which, given time, can crack most NT passwords. This note therefore gives guidelines on the generation and usage of passwords in order to reduce the possibility of them being cracked.

The following sections are rules intended to improve the quality of passwords. These rules have been approved by the Computer and Networks Security Group and users are required to take note of them and apply the advice without exception. Note also that the NT User's Code of Conduct (see *Annex 7: NT Users Code of Conduct*) contains instructions regarding passwords.

Rules for NT Passwords

For normal user passwords the following rules should apply:

Passwords must be at least 8 characters long. The maximum for NT is 14 characters.

Passwords must contain at least two different characters from each of the following 3 groups and no more than 3 adjacent characters may be members of the same group:

Letters in upper or lower case	A - Z
Numbers	0-9
Non-alphanumeric characters	- = [ ] \ ; ' , . / ` ~ ! @ # $ % ^ & * ( ) _ + { } | : " < > ?

Passwords must not be based on words or initials easily associated with you or your job. Thus your user name, initials, any part of your full name or any description related to your job function are not allowed.

A password must be changed whenever it becomes known to someone else who has no legitimate requirement to know it or who might represent a security risk, however small the risk may be.

The same password can be used to access other CCLRC facilities. However this is not recommended where passwords are sent in clear text, for example for authentication of NFS disk mounts. Care may be needed in the choice of non-alphabetic characters since some systems may only allow a reduced set.

For non-CCLRC facilities you must not use the same password nor give your federal ID to any system requiring a user name for registration purposes.

Where more than one password is required then similar formats and character substitutions should be avoided.

It is recommended that passwords are changed annually.

For high security passwords the minimum length is increased to 10 (ideally it should be 14) and the password must contain at least 3 different characters from each group and no more than 2 adjacent characters may be members of the same group. Unless it is not technically possible the password must be changed annually.

General Advice on Passwords

The requirement for a password to be memorable yet difficult to guess or crack is a hard one to meet but quite possible given some thought and ingenuity. The following suggestions only scratch the surface in an area where originality is the key to success.

A common way to make a password memorable is to use a known word. However this is not allowed because dictionaries are freely available for most languages and programs to crack passwords using them are very quick. An obvious way round this is to use two words which would not normally be together in a dictionary. Unfortunately the advent of brute force password crackers which will test all combinations of a set of characters means that this is no longer acceptable. Hence the requirement to generate a password from a larger character set.

To make a password memorable it needs to have a base. This can either be a word, or better still words, or, even better, some other easily remembered or recalled set of characters. In order that the base cannot be guessed by someone else it should not be something easily associated with you. Thus anything to do with the names of you or your family, your job or your favourite pass-time are not recommended unless the connection is obscure. Whilst your own initials are not allowed, those of grandparents or another distant relative or friend are acceptable. Similarly whilst the initials of your own address are not recommended those of grandparents etc. are also quite acceptable. The initials or shortened name of a charity you support or club of which you are a member are also a good starting point though try not to choose one which is common within CCLRC such as "recsoc". The first letters of a favourite line of poetry or prose is another possibility. If you always work in the same place there are many labels and other text strings around that can help. For example DCEPOSOIE is the first letters of the "Desktop Computer Equipment Powered Overnight Switch Off in Emergency" black label. Another possibility is the model number on an item of equipment such as VIGIV/33 on a Viglen computer. Yet another is the initials from the title of a book or manual on your office shelves. However care is needed where many people have the same type of equipment, labels etc. in their offices so could thus guess your password.

Since the base rarely conforms to the CCLRC password rules some means of transforming it is now required. A common technique has been to substitute the digit 1 for the letter i and the digit 0 for the letter o. However this is not recommended because it is so well known that some cracking programs now have this substitution built in to their dictionary checking mechanism.

But if this technique is extended by substituting one or more numbers or non-alphanumerics for some letters then a strong and memorable password is still possible provided obvious substitutions are avoided. Thus whilst an easy way of modifying the password "mygarden" is to make it "m1g@rd[n" perhaps a better one would be "m&g^rd/n" or even better "m&g^rd/n$" which is no longer just a word but still memorable since the $ reminds you that gardening can an expensive hobby. Don't however use a £ since it is not in the permitted character set.

Another valid technique is to take a base and add in some extra numbers and non-alphabetic characters. Hence "collect" could become "co+ll8ect=" and "in my day" could become "in#my7day!".

However a much better method is to add non-alphabetic characters to a base which is a set of initials since this takes something already obscure and adds further obscurity. Thus, for example, starting with the name and address of a grandparent as Jill Mary Dobbs, 29 Gifforth Avenue this produces the initials "jmd29ga" and with added non-alphabetic characters it could become "jmd29~ga?", "jm’d29ga!" or "jmd[29ga}". Similarly a favourite pub, the George & Dragon, which was usually visited at about 8:27 in the evening could produce the initials "g&d@8:27" which, although within the rules, is perhaps a little obvious in the use of non-alphabetic characters. A better version could be "g=d!8>27".

Another convenient way of generating a password is to choose a combination of characters on the keyboard. Whilst this is a bad technique if adjacent keys are used it can produce strong passwords provided the key pattern is not obvious. A very good variation on this method is to choose a base and then apply a shifting rule to each key as it is typed in. For example if the rule was to use the key above and to the right then the word "mygarden" becomes "k7yw5r4j". Care is needed in the choice of words in order to generate a password within the CCLRC rules and it may be necessary to add one or more non-alphanumeric characters in order to conform such as "k7,yw5r4j#" in the above example. A less obvious shift rule is also a good idea. Whilst touch typists will prefer a consistent rule, such as up and two to the right, others may go for a variable rule, such as up and two to the right, down and two to the left, up and two to the right etc. If a move takes you off the edge of the keys then wrap round to the opposite edge and use of the shift key on non alphabetic keys will widen the potential character set. Thus with the shift rule of one up and two to the left with the shift key added to alternate non alphabetic keys then "mygarden" becomes "h5r}3w"g". Users of more than one PC are warned that keyboard layouts do vary and thus passwords should be checked on each keyboard before using this technique.

To save confusion it is becoming common to use the same password on all systems a person uses. However care is needed because some systems have limitations on what characters a password can contain. It is therefore best to try out your proposed password on systems other than NT to see if it is acceptable. Where only a limited character set is allowed then it is strongly recommended that a minimum 10 character password is used.

Finally it is wise to give some thought when you use the same password for accessing different CCLRC facilities in order to minimise the damage if one is cracked. Thus it would be unwise to use your federal ID password to also authenticate your user name for an NFS disk mount especially if the former gives you access to sensitive data. This is because the NFS authentication is sent across the network in clear text and easily read by a sniffer. For the same reason the federal ID password is not recommended for an account accessed via Telnet or used for FTP access.

Further Reading

Anyone requiring further details of password cracking should consult the following documents:

General advice for unix systems
http://www.cert.org/tech_tips/passwd_file_protection.html

How passwords are stored in unix systems
http://www.itworld.com/nl/unix_sec/12132001/

User Authentication with Windows NT. Microsoft Knowledge Base
http://support.microsoft.com/support/kb/articles/Q102/7/16.asp

Annex 6: NT Administrators Code of Conduct

Initial Observations

An NT Domain Administrator is someone who knows the password to an account which is a member of the Domain Administrators' group.

The Administrator's Code of Conduct includes all aspects of the User's Code of Conduct (see below) with the added responsibility that the administrator is the authorised person trusted with giving users additional privileges. As such they need to accept their share of the responsibility for safeguarding the integrity of the CCLRC computing infrastructure, and apply their professional judgement before agreeing to make additional privileges available to any user.

The particular administrative privileges granted to a user should be sufficient for him to do the job required and no more. Thus, where possible, a subset of the full administrative privileges should be given. However such granularity is often not available since, although technically feasible, the lack of suitable tools to administer it make implementation impracticable.

Administrators have very wide-ranging powers which potentially enable them to access information held in any user's files. They are trusted not to access user-owned information unless absolutely necessary, and the permission of the owner must always be sought before doing so, or, if not immediately available, the owner must be informed at the earliest opportunity. Administrators must always confine their activities to those parts of the system pertinent to the job in hand. In particular they should be especially circumspect when it is necessary to look at files, network traffic or elsewhere which might contain private or confidential information. No use must be made of any information, such as a password, gleaned in this manner.

The line management of administrators must review this privilege at intervals.

Administrator Code of Conduct

The following guidance should be followed by all NT Domain Administrators.

1. The administrator will not reveal any of the passwords or permit accounts with administrative privilege to be used by anyone else without prior permission from their line management or other appropriate manager.
2. Passwords on accounts with Administrator privilege should be changed regularly or immediately if there is a security exposure. An exception to this is where a service needs to know the password and an example would be SMS.
3. Where possible the built-in Administrator account should not be used to change the rights of other users. Instead a user account that is a member of the Domain Administrators' group should be used so that the audit log can identify the person making the changes.
4. An administrator will not change or modify the auditing settings or clear the audit logs of the server such that the actions of administrators will not be logged except where such action is needed to keep the system running.
5. An administrator should consider very carefully, consulting their management where necessary, before giving additional privileges to users, especially when requested to make them an Administrator of their own PC or workstation. They should only be given to meet a specific requirement which the Domain Administrator accepts is fully justified and be removed when the need has passed.
6. An administrator should only use the privilege to read confidential or private information when it is absolutely necessary. It is a breach of this code of conduct for an administrator to read, modify, make use of or pass on, any information gleaned in this manner unless instructed to do so by the owner of the information or a more senior manager.

7. An administrator should confine usage of accounts with the Administrator privilege to only those tasks directly involved with administration. Such an account should not be used for any activity that could give rise to a security exposure. In particular activities such as reading e-mail and FTPing files from remote sites should be avoided due to the possibility of catching a virus.
8. It is not recommended that contractors be given Domain Administrator privileges, but if this is unavoidable this Code of Conduct should be incorporated in their contract.

Guidelines for Managers whose Staff Have Administrator Privilege

The requirement for an account to have the Domain Administrator privilege and for individuals to know the passwords should be reviewed regularly or when the password is changed.

The auditing levels should be set to detect any breach of security. Security logs should be monitored by managers at intervals not exceeding 3 months.

Annex 7: NT Users Code of Conduct

Initial Observations

Computing facilities can be classified into two categories. The first is that of general computing as exemplified by the CLEO applications and the second covers specific implementations such as the ISIS facility. Codes of conduct for the latter need to be very specific about permitted use and the need to constrain the user within strict bounds. As such they are outside the scope of this Code. Codes of conduct for more general computing can be somewhat more relaxed about usage and more general in their statements. An element of common sense is usually required in their interpretation.

A factor that must always be considered is the prevailing employment codes of conduct. Within CCLRC these come under CEM 8 on conduct and discipline and CCLRC Notice 26/96, November 1996, which covers issues relating to the use of computers and networks. The CEMs do not attempt to cover every aspect of personal behaviour as CCLRC prefers to rely on the good sense and integrity of its employees. Codes of conduct need to reflect this position.

Whilst an official document or web page describing a code of conduct carries sufficient authority to ensure compliance by CCLRC staff in general, there are other applications of computers where a tighter control of the users' actions might be more appropriate, for example, where external users have access to CCLRC's facilities or where access to sensitive data or safety systems is involved. In such cases a document signed by each user would carry more weight and should be considered.

User Code of Conduct

The following points apply to all information systems and to all users of those systems whether or not they are CCLRC employees. The term "authorised person" applies to any responsible person or persons appointed by individual departments for the purposes of this code.

1. The user will not reveal any of their passwords or permit their accounts to be used by anyone else, unless this is made necessary by very exceptional circumstances. The user will take full responsibility for the actions of anyone using one of their accounts.

2. The user will not change or modify such settings on any PC or workstation that affect the security of the system or the ability of an "authorised person" to monitor, virus check, carry out an inventory or otherwise modify the system. If any of these settings inhibits the user's ability to do their job then written permission from an "authorised person" should be obtained for modifying such settings. This may make the user responsible for any consequences of such a change.

3. Should the user be given additional privileges, such as being given "administrator" rights on their own machine, then these should be used only for the purpose for which they were granted. A request for them to be removed should be made as soon as the need has ended.

4. All users should ensure that they hold appropriate licences for the software they run on the computers they use, including CCLRC computers being used at home. Unless the licence allows it they should not permit the copying of software by unauthorised persons.

5. The user should take reasonable steps to ensure that anything passed on to other users or put in a public or shared area does not adversely affect other users. In particular it should be checked for computer viruses. The user will be held responsible for the consequences of failing to take such actions.

6. The user should not abuse shared resources, such as networks or file servers, in such a manner as to adversely affect other users. Where heavy usage is required as part of their job then it must be sanctioned by an "authorised person" and done in such a manner as to minimise the impact on other users. Users should be aware of the adverse effect on other users of doing large backups over the network.

7. Usage of computer networks must be within the limits of CCLRC Notice 26/96, November 1996 or any subsequent update. In particular this covers the creation or transmission of anything that is

offensive, obscene, indecent, defamatory or could cause annoyance or needless anxiety. It deems unacceptable any action that damages or disrupts the work of other users or violates their privacy.

8. Users with desktop equipment in their offices should be aware of the danger of fire. Units with a fire hazard, in particular monitors and laser printers, must not normally be left powered on unattended out of normal office hours. Other units with less of a fire hazard, such as system units, may be left powered on.

Annex 8: Network Acceptable Use Policy

JANET acceptable use policy

Almost all electronic communications between CCLRC and the outside world, including e-mail and access to the Internet and the World Wide Web, pass across the Joint Academic Network, JANET. It is a condition of the use of JANET that we comply with UKERNA's policy on acceptable use, a copy of which is shown below.

Your attention is drawn particularly to paragraph 9 which sets out the following modes of use which are **unacceptable:**

2.1. the creation or transmission (other than for properly supervised and lawful research purposes) of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;

2.2. the creation or transmission of material which is designed or likely to cause annoyance, inconvenience or needless anxiety;

2.3. the creation or transmission of defamatory material;

2.4. the transmission of material such that this infringes the copyright of another person;

2.5 the transmission of unsolicited commercial or advertising material either to other User Organisations, or to organisations connected to other networks, save where that material is embedded within, or is otherwise part of, a service to which the member of the User Organisation has chosen to subscribe;

2.6 deliberate unauthorised access to facilities or services accessible via JANET;

2.7 deliberate activities with any of the following characteristics:

> wasting staff effort or networked resources, including time on end systems accessible via JANET and the effort of staff involved in the support of those systems;
>
> corrupting or destroying other users' data;
>
> violating the privacy of other users;
>
> disrupting the work of other users;
>
> using JANET in a way that denies service to other users (for example, deliberate or reckless overloading of access links or of switching equipment);
>
> continuing to use an item of networking software or hardware after UKERNA has requested that use cease because it is causing disruption to the correct functioning of JANET;
>
> other misuse of JANET or networked resources, such as the introduction of "viruses".

This policy will be applied to the use of JANET and by analogy to the use of all telecommunications networks and facilities available within CCLRC, including internal networks.

All staff are required to adhere to the policy. Failure to do so on the part of individuals will invoke disciplinary procedures.

Chat lines and newsgroups

The use of chat lines and of Usenet alt (controversial or unusual topics) class newsgroups is banned, unless a specific case is made to and agreed by a Department Head on the grounds of relevance to the work of the Council. Automatic barring will be introduced as far as resources and techniques permit.

Random monitoring

Monitoring of computer network traffic is regulated in the UK by the Regulation of Investigatory Powers (RIP) Act. As a matter of policy, CCLRC will comply with the provisions of the RIP Act. CCLRC will monitor the use of JANET and CCLRC internal telecommunications networks, both to provide assurance that CCLRC staff (and users of CCLRC facilities) are complying with the acceptable use policy and to ensure that there is no illegal use of these networks.

Monitoring will be carried out by sampling network traffic, principally but not exclusively at the junctions between the CCLRC internal networks and JANET, by properly authorised staff. This may include the inspection of traffic data and, when justified and legally permitted, the content of all network traffic, including web accesses and e-mail.

Conditions of employment memoranda (CEMs)

The provisions of CEM 8 on conduct and discipline apply as much to the use of computers and networks as to other aspects of the Laboratory's work. The CEMs and do not attempt to cover every aspect of personal behaviour as the Council prefers to rely on the good sense and integrity of its employees.

However, you are reminded that it is a condition of your employment that you should not engage in behaviour or activities likely to bring discredit on the Council, and that Council property, equipment and facilities may be used only for authorised purposes (CEM 8A paragraphs 2.1.1 and 2.1.3). Breach of this condition may give rise to disciplinary action.

This Notice has been agreed by the Trade Union Side.

UKERNA JANET Acceptable Use Policy

Version 6.0

April 2001

Trademarks:

"JANET" and "UKERNA" are trade marks of the Higher Education Funding Councils for England, Scotland and Wales, which have granted the JNT Association the right to use the marks.

Disclaimer:

Neither the Higher Education Funding Council for England nor the JNT Association can accept any liability for any loss or damage resulting from the use of the material contained herein. The information is believed to be correct but no liability can be accepted for any inaccuracies.

Availability:

Further copies of this document may be obtained from the JANET Liaison Desk, UKERNA, Atlas Centre, Chilton, Didcot, Oxfordshire, OX11 0QS.

Background and Definitions

1. "JANET" is the name given to the collection of networking services and facilities which support the communication requirements of the UK education and research community.

2. The Higher Education Funding Councils for England, Scotland and Wales, the Learning and Skills Council, the Scottish Further Education Funding Council, the National Council for Education and Training for Wales and the Department of Higher and Further Education, Training and Employment are responsible jointly for the provision of JANET. They exercise this responsibility through their Joint Information Systems Committee (the JISC) and any dispute over the interpretation of this Policy will be resolved by the JISC.

3. UKERNA (an acronym for the United Kingdom Education and Research Networking Association) is the trading name of the company contracted by the JISC, acting in the name of the Higher Education Funding Council for England, for the provision of the JANET service. This includes the day-to-day management of this Policy.

4. This Policy applies in the first instance to any organisation authorised to use JANET (a "User Organisation"). It is the responsibility of User Organisations to ensure that members of their own user communities use JANET services in an acceptable manner and in accordance with current legislation.

5. It is therefore recommended that each User Organisation establishes its own statement of acceptable use within the context of the services provided to its users, and in a form that is compatible with the conditions expressed in this Policy. Such a statement may refer to, or include, this document. If material from this document is included, this must be done in such a way as to ensure that there is no misrepresentation of the intent of this Policy. UKERNA can advise on this aspect as and where necessary.

6. JANET is maintained to support teaching, learning and research. The connection of any organisation to JANET is governed by the JANET Connection Policy maintained by the JISC.

Acceptable Use

7. A User Organisation may use JANET for the purpose of interworking with other User Organisations, and with organisations attached to networks which are reachable via interworking agreements operated by UKERNA. All use of JANET is subject to payment of the appropriate charges in force during the period of service. Any provision of service must be authorised in advance.

8. Subject to the following paragraphs, JANET may be used for any legal activity that is in furtherance of the aims and policies of the User Organisation.

Unacceptable Use

9. JANET may not be used for any of the following:

9.1. the creation or transmission (other than for properly supervised and lawful research purposes) of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;

9.2. the creation or transmission of material which is designed or likely to cause annoyance, inconvenience or needless anxiety;

9.3. the creation or transmission of defamatory material;

9.4. the transmission of material such that this infringes the copyright of another person;

9.5. the transmission of unsolicited commercial or advertising material either to other User Organisations, or to organisations connected to other networks, save where that material is embedded within, or is otherwise part of, a service to which the member of the User Organisation has chosen to subscribe;

9.6. deliberate unauthorised access to facilities or services accessible via JANET;

9.7. deliberate activities with any of the following characteristics:

wasting staff effort or networked resources, including time on end systems accessible via JANET and the effort of staff involved in the support of those systems;

- corrupting or destroying other users' data;

- violating the privacy of other users;
- disrupting the work of other users;
- using JANET in a way that denies service to other users (for example, deliberate or reckless overloading of access links or of switching equipment);
- continuing to use an item of networking software or hardware after UKERNA has requested that use cease because it is causing disruption to the correct functioning of JANET;
- other misuse of JANET or networked resources, such as the introduction of "viruses".

10. Where JANET is being used to access another network, any abuse of the acceptable use policy of that network will be regarded as unacceptable use of JANET.

Passing on and Resale of JANET Service

11. It is not permitted to provide access to JANET for third parties without the prior agreement of UKERNA, with the exceptions in the following sub-paragraphs.

11.1. The JISC has resale schemes whereby certain types of User Organisation may sell on JANET services under defined circumstances. Details may be obtained from UKERNA.

11.2. It is acceptable for a User Organisation connected to JANET to extend access to others on a limited basis, provided no charge is made for such access. For example, it is acceptable that a visitor to the Organisation be permitted to gain access to JANET for the purpose of maintaining contact with his or her home organisation. It is intended that such use be regulated by the User Organisation in the same manner as it would regulate occasional use by third parties of its other facilities, such as its telephone and IT support systems.

12. A third party, where an individual, means someone who is not acting as a member of the User Organisation. Where it applies to a separate organisation, this is defined to be any organisation that is in law a separate entity to the User Organisation.

Compliance

13. It is the responsibility of the User Organisation to take all reasonable steps to ensure compliance with the conditions set out in this Policy document, and to ensure that unacceptable use of JANET does not occur. The discharge of this responsibility must include informing those at the Organisation with access to JANET of their obligations in this respect.

14. Where necessary, service may be withdrawn from the User Organisation. This may take one of two forms.

14.1. An indefinite withdrawal of service, should a violation of these conditions persist after appropriate warnings have been given by UKERNA. Such a withdrawal of service would only be made on the authority of the JISC. Restoration would be made only when the JISC was satisfied that the appropriate steps had been taken at the Organisation involved to ensure acceptable behaviour in future.

14.2. A suspension of service, should a violation of these conditions cause serious degradation of the service to other users of JANET. Such a suspension would be made on the judgement of UKERNA, and service would be restored when the cause of the degradation of service to others had been removed.

15. Where violation of these conditions is illegal or unlawful, or results in loss or damage to UKERNA or JANET resources or the resources of third parties accessible via JANET, the matter may be referred for legal action.

16. It is preferable for misuse to be prevented by a combination of responsible attitudes to the use of JANET resources on the part of users and appropriate disciplinary measures taken by their Organisations.

Annex 9: RAL LAN Managers

The RAL LAN Managers in July 2002 were:

Village Name	Manager
Administration	R S Owen, R Metcalf
Engineering	M J D Courthold, M Rudman
Applied Science (Micro)	P J Hallowell, M Rudman
Chilbolton	D Ladd
BITD	R Brandwood, N Moore
Particle Physics	B Saunders, D Kelsey, G R Smith
ISIS (Cntrl)	R Brodie, R P Mannix
ISIS (Neutron)	A Valente, F.Akeroyd, K Knowles
Lasers	C J Reason
ISIS (Science)	J R Hogston, K Brine
Space (AG)	P Chiu, M Kendall
Space (BNSC/SDC)	A Boulter, D Russell
Space (STP)	M Wild, P Gallop
TechElec	A J Lucas, N K Watkins
EBW	R J Young, A M Shepherd
E-Science	N Hill, R A Sansum

An up-to-date list together with contact details can be found at **http://netweb.rl.ac.uk/vill.php**

Note that the earlier departments of Applied Science, Technology and Computation and Information have been reorganised, although the underlying network ‘villages’ remain largely unchanged.

Annex 10: Email Postscripts

Disclaimers

The following texts are recommended for appending to email being sent off-site as disclaimers which would provide a small measure of protection against mis-direction, interception, copyright violation or defamation. Users are free to choose the most appropriate of the two texts for the particular email being sent. The text should normally be appended at the foot of the email after the sender's "signature".

Insert either:

“The contents of this email are sent in confidence for the use of the intended recipient only. If you are not one of the intended recipients do not take action on it or show it to anyone else, but return this email to the sender and delete your copy of it.”

Or:

"This email represents the opinion of the author only and should not be construed as reflecting CCCLRC's corporate view."

Monitoring

To enable the interception of email for purposes other than operating the email system itself in a way that complies with the RIP Act it is necessary to take all reasonable steps to inform potential senders of email that monitoring may occur. This is best achieved by appending a message to the end of all outgoing emails which says:

“CCLRC’s telecommunications systems may be monitored in accordance with the policy available from http://www.foi.cclrc.ac.uk/Activity/ACTIVITY=Monitoring”.

Annex 11: Data Protection Principles

The eight Data Protection Principles are specified fully and interpreted in Schedule I to the Data Protection Act 1998. In summary, they are:

1 *Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless certain conditions are met*

2 *Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes*

3 *Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed*

4 *Personal data shall be accurate and, where necessary, kept up to date*

5 *Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes*

6 *Personal data shall be processed in accordance with the rights of data subjects under this Act*

7 *Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction, or damage to, personal data*

8 *Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.*

Some pertinent definitions taken from the Act are:

Data means information which

a) is being processed by means of equipment operating automatically in response to instructions given for that purpose,

b) is recorded with the intention that it should be processed by means of such equipment,

c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, or

d) does not fall within paragraph (a), (b) or (c) but forms part of an “accessible record” defined in the Act to include certain health, educational and public records.

Personal Data means data which relate to a living individual who can be identified

a) from those data, or

b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Data Controller means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

Annex 12: LAN Managers' Code of Conduct

Initial Observations

A LAN Manager (also known as a Village Manager at RAL) is someone who is entrusted to manage a section of the CCLRC physical data network, often lying within a Department or part of a Department.

LAN Managers are the persons authorised within CCLRC to give users access to the data network. As such they need to accept their share of the responsibility for safeguarding the integrity of the CCLRC network infrastructure. They must apply their professional judgement before taken any action which might affect network integrity, especially when agreeing to make additional privileges for accessing the network available to others. If others are given these additional privileges they must be made aware of this Code of Conduct and undertake to follow it.

LAN Managers have very wide ranging powers which potentially enable them to access information traversing both the data and telecommunications networks. They are trusted not to access user-owned information unless absolutely necessary. LAN Managers must always confine their activities to those parts of the data network for which they are responsible. In particular they should be especially circumspect when it is necessary to look at network traffic that might contain private or confidential information. No use must be made of any information, such as passwords, gleaned in this manner. They have no right of access to the telecommunications network or the traffic it is carrying.

The line management of LAN Managers must review the assignment of this privilege at intervals.

LAN Managers' Code of Conduct

The following guidance should be followed by all LAN Managers.

1. LAN Managers will ensure that major components of the data network are located in a secure environment.
2. The Wiring Closets to which LAN Managers have access may also contain telecommunications equipment and wiring. They are not permitted access to this equipment and they must ensure they are familiar with the wiring labelling and allocations in order to limit their activities to the wiring currently in use for data.
3. Access to Wiring Closets should be given only to trusted staff who are aware of their responsibilities and have understood and accepted this Code of Conduct. LAN Managers must be always be aware of the scope of the work that is being undertaken on their behalf by others.
4. LAN Managers should limit their actions and those of staff they appoint to the data network for which they are responsible. That part of the physical network which carries telecommunications traffic is out of bounds to LAN Managers and those they appoint.
5. LAN Managers must ensure the safe keeping of any keys or security codes given to them.
6. LAN Managers must follow any additional CSTOB, CNSG or LMC guidelines relating to wiring management.
7. LAN Managers should limit network connections and allocation of network addresses to those who need them for the benefit of CCLRC.

It is not recommended that contractors be given unsupervised access to the wiring, but if this is unavoidable then clear instructions must be given to ensure this Code of Conduct is followed.

Annex 13: The Regulation of Investigatory Powers (RIP) Act 2000

This section is taken largely from advice prepared by the JISC Legal Information Service http://www.jisc.ac.uk/legal

Key Issues

Interception of communications on an institution's own telecommunications network, including computer communications such as email, is unlawful unless it is carried out in accordance with the RIP Act 2000 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

Unlawful interception on an institution's own telecommunications networks may lead to criminal sanctions against an individual operating without the institution's authority.

Unlawful interception on an institution's own telecommunications networks may lead to civil action against the institution where the institution authorised the interception.

The RIP Act 2000

The RIP Act received Royal Assent in July 2000 and came into force in October 2000. It covers the interception of communications made via public postal systems, public telecommunications systems and private telecommunications systems.

Public telecommunications systems are any "telecommunications service which is offered or provided to, or to a substantial section of, the public in any one or more parts of the United Kingdom".

A private telecommunications system is any telecommunications system which is not a public telecommunications system but is attached to such a system.

The RIP Act makes it a criminal offence to "intentionally and without lawful authority" intercept any communication in the course of its transmission by public postal or telecommunications systems or private telecommunications systems. Interception on a private telecommunications system, however, is not a criminal offence where the person intercepting the communication is a person with a right to control that system or one who has express or implied permission to intercept communications on that system. In these circumstances the interception may, if made "without lawful authority", give rise to civil action.

Legitimate Private Interceptions

The RIP Act provides "lawful authority" for interceptions through exceptions included in the Act or in the rules to be found in the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

A ***general exception*** is made in the Act for interception where the interception is made by, or on behalf of, a person running the telecommunications service for purposes connected with the provision or operation of that service. Thus email postmasters may examine mis-addressed messages in order to redirect them, and to check for viruses held within them. Similarly, system operators may monitor traffic to determine its source, for example to eliminate unsolicited commercial email. The Act imposes no requirement on the telecommunications service operator to to give warning of the possible loss of privacy which may occur as a consequence of these interceptions.

The ***Telecommunications Regulations*** cover interceptions made by or with the consent of a person carrying on a business, for purposes relevant to that business, and on that business's own telecommunications system. They define the circumstances under which communications made be monitored and recorded, or only monitored.

Institutions may monitor and record communications:

- To establish the existence of facts to ascertain compliance with regulatory or self-regulatory practices or procedures or to ascertain or demonstrate standards which are or ought to be achieved
- In the interests of national security
- To prevent or detect crime
- To investigate or detect unauthorised use of telecommunications systems
- To secure, or as an inherent part of, effective system operation.

Institutions may monitor but not record:

- Received communications to determine whether they are business or personal communications
- Communications made to anonymous telephone help-lines

Notice of interceptions

Interceptions made under the authority of the Telecommunications Regulations will only be lawful if the controller of the telecommunications system on which they occur has made all reasonable efforts to inform potential users that interceptions may be made.

Annex 14: Authority to Intercept Communications

To conform with the RIP Act any person intercepting telecommunication messages on private telecommunications systems must have lawful authority to do so.

This may be implied by the exception in the RIP Act which permits interception by the person running a telecommunications service, or someone acting on his behalf, for purposes connected with the provision or operation of that service, but it is strongly recommended that this be not relied upon, and to ensure that written authority is in place as described below.

Written authority may be provided by the CCLRC IS Security Officer, the Deputy IS Security Officer, the Department Security Officer (DSO), or by the appropriate Departmental IS Security officer for those parts of the telecommunications systems under his/her control. It should take the following form:

"<Name> is hereby authorised to intercept communications on the <identify which part of the telecommunications systems> for the purposes of <one of the lawful purposes defined by the Act> for the period <from date> to <to date>.

"Signed <signature> (<Official title>)

The period should not exceed 1 year.

The authorising officer should hand the authorised person the original of the authorising form, retaining a copy and forwarding a copy to the CCLRC IS Security Officer.

The IS Security Officer will maintain a file of all such authorisations.

Appendix B: Document Control

Document Location

http://www-internal.clrc.ac.uk/staff/computing/security/issue2.0.doc

Change Control

Last saved by T Daniels on 24/07/2002 13:49

Version	Date	Author	Purpose	Audience
Draft A	31 Dec 98	T Daniels	For internal comment	BWD, PSK, MCC
Draft B	12 Jan 99	T Daniels	For formal comment	CNSG, RCIAS
Draft C	7 Mar 99	T Daniels	For approval	CNSG, RCIAS
Draft D	9 Apr 99	T Daniels	Incorporates CNSG changes. For approval and adoption	RCIAS, LMB
Draft E	9 Apr 99	T Daniels	Incorporates changes notified after 9 Apr. For approval and adoption	RCIAS, LMB
Issue 1	19 Jul 99	T Daniels	For issue following LMB and RCIAS ratification	All CCLRC Staff and contractors on site
Issue 1.1	1 March 00	T Daniels	Change email, modems; add Village Managers CoC	All CCLRC Staff and contractors on site
Issue 2.0 Draft A	10 Jan 2002	T Daniels	Complete revision of detail; add RIP Act, home computers, wireless LANs for CNSG consideration.	CNSG
Issue 2.0 Draft B	29 Jan 2002	T Daniels	Incorporate comments from CNSG for BSSG consideration	BSSG
Issue 2.0 Draft C	26 Mar 2002	T Daniels	Incorporate comments from BSSG for AC, RCIAS and CMB consideration and ratification	AC, RCIAS and CMB
Issue 2.0	24 July 2002	T Daniels	Bring factual details up to date ready for issue, following CMB ratification	All CCLRC staff and contractors on site